FUJ00087227

Confidential and subject to litigation privilege

ALAN BATES & OTHERS v POST OFFICE LIMITED

Briefing for Fujitsu

1. PRIVILEGE

1.1 This briefing has been prepared for the purpose of seeking Fujitsu's assistance in preparing Post Office's case in the above litigation. This document, and all related or connected documents, are also privileged

2. OVERVIEW

2.1 A group of current and former postmasters (**Claimants**) have brought a claim against Post Office (the **Group Litigation**). Post Office has provided Fujitsu with four key letters that have been exchanged between the Claimants' lawyers (**Freeths**) and Post Office's lawyers (**Bond Dickinson**) and Freeths' "generic" Particulars of Claim. As is made clear from these documents, the Claimants have made of a number of allegations that the Horizon system is defective and the processes associated with it are inadequate.

2.2 One such allegation is that Post Office / Fujitsu has the ability to add / delete / change transactions recorded by branches without the consent / knowledge of a postmaster and that this may have been the cause of discrepancies in some of the Claimants' branch accounts. This has become known, perhaps inaccurately, as the "remote access" issue. This issue has been formulated in several different ways by the Claimants:-

2.2.1 Post Office / Fujitsu have the ability to log on remotely to a Horizon terminal in a branch so to conduct transactions.

2.2.2 Post Office / Fujitsu have the ability to conduct transactions (either remotely or locally) under another user 's ID,

2.2.3 Post Office / Fujitsu have the ability to push transactions into a branch's accounts without either a postmaster's (a) knowledge or (b) consent.

2.2.4 Post Office / Fujitsu have the ability to amend or delete transactions entered by branch staff on Horizon (and can do so in a way that is hidden from postmasters).

2.3 Post Office instructed Deloitte to plan and execute procedures to provide assurance that the Horizon system operates as expected, and there are reasonable controls and safeguards in place to prevent incorrect system operation that could have resulted in postmaster detriment, in relation to remote access. Deloitte's findings to date are summarised in section 2 below. In short, Deloitte has found that a limited number of authorised Fujitsu personnel (**Super-Users**) have sufficient privileges to theoretically edit and/or delete transactions in the Branch Database and although Horizon is designed in such a way that "Super-user activity" should leave behind a footprint showing that changes had been made to transaction data, it is thought that certain Super-Users may have sufficient access rights to cover their tracks so that no log / footprint of the changes would be left behind (i.e. a lack of segregation of duties).

2.4 Fujitsu has offered to provide a comprehensive paper that details the measures and protections in place to ensure that the risk of a Super-User altering transaction data so as to cause a discrepancy in a postmaster's branch accounts, and cover their tracks, is theoretical only.

2.5 It should be noted that for the purposes of the Group Litigation it is not sufficient for Post Office to state that there is no evidence to suggest that there has never been an attempt to use the Super-User facility to affect branch accounts outside of any proper and agreed process. The specific questions that Post Office needs to address in order to meet the Claimants' allegations in relation to remote access as they currently stand are set out in section 3 below. The

FUJ00087227

Confidential and subject to litigation privilege

Claimants may seek to refine and / or augment those allegations as the Group Litigation progresses, which may lead to Post Office having to answer further questions.

3. SUMMARY OF DELOITTE'S FINDINGS REGARDING REMOTE ACCESS TO DATE

3.1 As branch accounts draw on data from the Branch Database additions, edits or deletions in the Branch Database could impact upon branch accounts.

3.2 On a review of relevant technical documentation Deloitte identified the following key controls which are stated to regulate Super-User activity in Horizon Online:-

3.2.1 Counter transactions are given a unique JSN of 1 greater than the previous transaction so that the completeness (density) of the flow of transactions from a particular branch can be checked when data is extracted from the Audit Store. They are also digitally signed (i.e. a unique "hash" is applied to each message) so that the accuracy and validity of the message can be checked;

3.2.2 the interface files in respect of non-Counter transactions, which are inserted into the Branch Database when a Transaction Acknowledgment is accepted by branch staff, are also sent directly to the Audit Store which allows for reconciliation between the two data sources when data is extracted from the Audit Store;

3.2.3 when data is taken from the Branch Database to the Audit Store via the Audit Server it is sealed (while in the Audit Server) and a database of sealed files is maintained so that when data is subsequently retrieved from the Audit Store, its integrity can be checked;

3.2.4 upon receipt of data files retrieved from the Audit Store POL investigators carry out checks to validate data integrity (it should be noted that the nature of these checks was outside the scope of Deloitte's work);

3.2.5 Super-User activity is logged; and

3.2.6 Super-Users cannot amend activity logs, JSNs, invalidated digital signatures or invalidated digital seals (i.e. they cannot cover their tracks).

3.3 Although digital signatures did not exist in Legacy Horizon, a "CRC check" was applied which would notify Fujitsu if any amendments had been made to data when it was retrieved from the Audit Store if operating correctly. Fujitsu represented to Deloitte that controls surrounding the Audit Store have remained largely unchanged.

3.4 A branch would not be notified if a Super-User amended or deleted a transaction. However, if a change was made in the Branch Database:-

3.4.1 before a record of it was "collected" by the Audit Server (which typically happens every 15 minutes), the edition/deletion would track through to the Audit Store. However, if data was subsequently obtained from the Audit Store:

(a) for Counter transactions: (1) deletions would be revealed by the "data density" check (JSNs)and (2) edits would be revealed by invalidated digital seals and signatures; and

(b) for non-Counter transactions: (1) the completeness and validity of data could be checked by reference to interface files.

3.4.2 after a record of it had been "collected" by the Audit Server it would not impact on the record of the transaction in the Audit Store and there would therefore be a discrepancy

FUJ00087227

Confidential and subject to litigation privilege

between the branch accounts (being the record in the Branch Database) and data subsequently obtained from the Audit Store.

3.5 Deloitte carried out certain tests in order to provide assurance as to whether the controls identified in the technical documentation operate effectively in practice. It was noted that:-

3.5.1 certain Super-Users can amend JSNs, invalidated digital signatures and invalidated digital seals, although it is theorised that they would need to create a computer program to do this in view of the amount of work that would need to be done in a limited window;

3.5.2 the audit trail is only checked when transaction data is extracted from the Audit Store, which typically only happens when POL has cause to investigate specific issues / complaints raised by postmasters;

3.5.3 the data integrity checks that are carried out when data is extracted from the Audit Store can be ignored by Fujitsu staff; and

3.5.4 the audit trail in respect of Super-User activity is not pro-actively inspected.

Deloitte did not obtain and review the audit logs of Super-User access (the work was not originally commissioned as there was no indication of failure in the controls around Super-Users).

4. REMOTE ACCESS ISSUES TO BE ADDRESSED

4.1 The points below apply to both Horizon and Horizon HNG-X.

4.2 The key question is whether Horizon accurately and only records the transactions input or approved by branch staff in a manner that either:-

4.2.1 cannot be added to, deleted or altered; or,

4.2.2 if they can be added to, deleted or altered, such changes will, in all circumstances, be either:

(a) visible to postmasters; or at least

(b) logged and identifiable by Post Office / Fujitsu / a third party expert.

4.3 Assuming the above is correct, it should be possible to either:-

4.3.1 prove that no such changes occurred in a particular branch; or

4.3.2 where changes have occurred, identify such changes and show what changed.

4.4 The specific outstanding questions from Deloitte's work are:-

4.4.1 What exact information is logged by the Super-User Audit Logs?

4.4.2 Would this logged information show that:-

(a) a Super-User had done something that could change a branch's accounts in the real-world (e.g. that the Super-User had amended or deleted a transaction in the Branch Database); and

(b) what that Super-User had done (i.e. does it show the change in such a way that it could be identified and either isolated or reversed out)?

FUJ00087227

Confidential and subject to litigation privilege

4.4.3 If the Super-User Audit Logs would not reveal all actions by Super-Users that could affect branch accounts, please provide a full description of ways in which a Super-User could amend a branch's accounts in a way that could would not leave behind a footprint of their activity is required.

23 February 2017